NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

Chapter 3 IT Program and System Security Assessments

3.1 IT Program and System Security Assessments Overview

3.1.1 FISMA requires NASA to conduct annual IT security assessments of systems and programs and reviews of Centers and contractor operations or facilities that process, store, or handle NASA information, and parties under grants, agreements, or partners via volunteer or special agreements that process, store, or handle NASA information.

3.1.2 A "contractor operation or facility" is an entity under contract or other government agreement that processes or stores NASA information or data and is managed by the entity with little government technical oversight of its operations. This includes, but is not limited, to a government-owned, contractor-operated (GOCO) facility, an outsourced function, a grant, or agreement from NASA to a college, university, or research facility to process, use, or be afforded access to Federal or NASA information or data.

3.2 IT Program and System Security Assessment Requirements

3.2.1 All IT program and system security assessments shall be coordinated with managers at the appropriate level (i.e., the NASA OCIO, Center CIO, Center ITSM, or the Procurement Officer) to ensure that critical business and mission functions are not disrupted and contractual provisions provide for assessments in place.

a. All non-NASA systems containing NASA information that is categorized as having

high impact to the NASA mission or operations shall have an assessment completed once every fiscal year under the oversight of the NASA CIO or Center CIO, as appropriate.

b. All NASA information system owners shall ensure that the appropriate reviews and testing as called for by NIST are conducted.

3.2.2 The necessary depth and breadth of an annual program or system assessment shall follow ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment, and ITS SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

3.2.3 Non-NASA performed IT program and system security assessments shall have an assessment that provides for:

a. Personnel screening equivalent to the information system's most stringent screening requirement, per NPR 1600.1, NASA Security Program Procedural Requirements, for all assessment team members.

b. Non-disclosure agreements previously approved by NASA General Counsel or Chief Counsel, to be signed by all entities and personnel participating in the assessment.

c. Protective controls for all materials, documents, working papers, and assessment findings at a level equivalent to that required by the information category.

d. The return or destruction of all materials, documents, working papers, and assessment findings at the completion of the IT program or system security assessment.

e. The assessment plan authorized and signed by the government sponsor of the assessment and the program manager of the non-NASA certifying entity responsible and accountable for the assessment prior to the start of the assessment.

3.2.4 Penetration testing conducted as part of any assessment shall adhere to ITS-SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

3.2.5 Federal and NASA non-compliance findings, which are not corrected or waived during the assessment, shall be entered into the program's or IT system's POA&M and be reported to the cognizant Contracting Officer and AO. The requirement to report non-compliance of a contractor's system shall be reported to the responsible civil service manager as well as all NASA Information Owners.

3.3 Additional IT Program and System Security Assessment References

a. OMB M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

b. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems.

c. ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

d. ITS SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

e. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS